Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of:	)	
	)	
Public Safety and Homeland Security	)	
Bureau Seeks Comment on Increasing Public	)	PS Docket No. 10-168
Safety Interoperability by Promoting	)	
Competition for Public Safety Communications	)	
Technologies	)	

COMMENTS OF
THE NATIONAL PUBLIC SAFETY TELECOMMUNICATIONS COUNCIL

The National Public Safety Telecommunications Council (NPSTC) submits these Comments in response to the Commission's Public Notice, DA10-1556, released August 19, 2010. This Public Notice advises that the importance of public safety communications makes it imperative that the Commission explore all potential barriers to achieving nationwide interoperability for both broadband and narrowband communications and determine what, if any, actions the Commission should take in this area.[1]

NPSTC provides the comments herein with the goals of bringing clarity to the issues of competition and interoperability in narrowband communications today and of reaffirming foundational steps that can enable competition and interoperability as the U.S. moves forward with deployment of public safety broadband networks. Competition and interoperability are both very important to public safety but increased competition alone does not improve interoperability. One of the most impactful factors on interoperability as we move forward with broadband is to avoid the fractured small slivers of spectrum across multiple bands that have defined narrowband systems.

[1] *See* Public Notice, DA 10-1556, PS DS Docket No. 10-168, released August 19, 2010.

The National Public Safety Telecommunications Council

The National Public Safety Telecommunications Council is a federation of public safety organizations whose mission is to improve public safety communications and interoperability through collaborative leadership. NPSTC pursues the role of resource and advocate for public safety organizations in the United States on matters relating to public safety telecommunications. NPSTC has promoted implementation of the Public Safety Wireless Advisory Committee (PSWAC) and the 700 MHz Public Safety National Coordination Committee (NCC) recommendations. NPSTC explores technologies and public policy involving public safety telecommunications, analyzes the ramifications of particular issues and submits comments to governmental bodies with the objective of furthering public safety telecommunications worldwide. NPSTC serves as a standing forum for the exchange of ideas and information for effective public safety telecommunications.

The following 15 organizations participate in NPSTC:

American Association of State Highway and Transportation Officials
American Radio Relay League
Association of Fish and Wildlife Agencies
Association of Public-Safety Communications Officials-International
Forestry Conservation Communications Association
International Association of Chiefs of Police
International Association of Emergency Managers
International Association of Fire Chiefs
International Municipal Signal Association
National Association of State Chief Information Officers
National Association of State Emergency Medical Services Officials
National Association of State Foresters
National Association of State Technology Directors
National Emergency Number Association
National Sheriffs' Association

Several federal agencies are liaison members of NPSTC. These include the Department of Homeland Security (the Federal Emergency Management Agency, the Office of Emergency Communications, the Office of Interoperability and Compatibility, and the SAFECOM Program);

Department of Commerce (National Telecommunications and Information Administration); Department of the Interior; and the Department of Justice (National Institute of Justice, CommTech Program). NPSTC has liaison relationships with associate members, the Telecommunications Industry Association, the Canadian Interoperability Technology Interest Group, and the Utilities Telecom Council.

NPSTC Comments

The Commission's Public Notice raises the following questions:

1. What are the factors that affect the current state of competition in the provision of public safety communications equipment? Are there any additional barriers to additional manufacturers supplying network equipment to the public safety community for narrowband communications? For broadband communications?

2. How would additional competition in the provision of public safety communications equipment improve narrowband or broadband interoperability? Conversely, what impact does the current state of competition in the provision of public safety communications equipment and devices have on interoperability? Assuming additional competition would benefit public safety interoperability, what actions could the Commission take to improve competition in the provision of public safety communications equipment?

3. What are the limitations of Project 25 in promoting narrowband public safety communications interoperability? What actions, if any, should the Commission take to rectify these limitations?

4. Could open standards for public safety equipment increase competition? What actions could the Commission take to facilitate openness?

5. As the Commission considers requirements for the 700 MHz broadband public safety network, are there any requirements on public safety equipment or network operators that would increase competition in the provision of public safety equipment? How can the Commission's work on requirements for the 700 MHz broadband public safety network be leveraged to promote interoperability between narrowband and broadband networks?

Given that there is significant overlap in NPSTC's input across several of the issues raised, we have organized our response to cover key points and avoid repeating the same information.

Current Public Safety Systems

Competition and interoperability are completely different factors in the market. In fact, the highest level of interoperability is normally achieved when only one provider serves the entire market, as evidenced by the wireline telephone industry prior to the breakup of the Bell system. However, interoperability is obviously not the only requirement for public safety. Competition and multiple sourcing are very important, just as products that meet operational requirements are essential.

Broadly defined, the public safety community performs emergency first-response missions to protect life, health, property, natural resources and to serve the public welfare. Emergency responders – police officers, fire personnel, emergency medical technicians, transportation and utility workers and others need to share vital voice and data information across disciplines and jurisdictions to successfully respond to day-to-day incidents and large-scale emergencies. Public safety operations require effective command, control, coordination, communication, and sharing of information via dispatch centers or Public Safety Answering Point (PSAP) responsible for answering emergency calls for police, firefighting, and ambulance services.

The key factor that affects the state of competition in the public safety market is the market size. Law enforcement, fire, and emergency medical personnel total approximately 2 to 3 million users. In addition, there are an estimated 6 to 9 million critical infrastructure users that also make up this market, bringing the total public safety and critical infrastructure market to an estimated 8 to 12 million users. In contrast, the consumer cell phone market in the U.S. totaled approximately 285 million at yearend 2009.[2] In other words, equipment vendors can choose to dedicate their

[2] http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use

resources to the specialized and demanding needs of the public safety market or apply those resources instead toward a consumer market that is 25 or more times larger.

While cost is certainly a factor for public safety, the lives of public safety personnel and the public they protect depend on communications solutions that can stand up to the rigor of the public safety environment and requirements that are much more demanding than the general consumer market. Therefore, the implication that public safety should just abandon their dedicated communications systems and use cell phones instead to save money completely ignores the key fact that cell phones designed for a consumer market do not meet public safety's critical requirements.

This issue was addressed recently by Bill Schrier, the CIO of the City of Seattle, who also co-chaired the Governance working group in the NPSTC Broadband Task Force. Mr. Schrier, a respected member of the public safety community, enumerated the following key reasons that public safety needs its own dedicated networks:[3]

- Priority. Cellular networks do not prioritize their users or traffic. A teenager's cell phone has the same priority as a cell phone used by a police officer or, for that matter, the BlackBerry used by President Obama. We've all experienced "no circuits available" or "network busy" when using a cell phone. When I'm being assaulted or have been injured in an automobile accident or even have had my house burglarized, the last thing I want is to have the network be "busy" so a police officer or EMT couldn't be dispatched. Public safety needs dedicated frequencies where police officers and firefighters have priority and even, perhaps, exclusive rights to use, without calls being clogged by the public.
- Reliability. Seattle's public safety radio network, part of the larger King County-wide 800 megahertz public safety radio network, handles more than 60,000 police, fire, and emergency medical calls every day. It operated last year with 99.9994% reliability - that's about 189 seconds of downtime out of more than the 31 million seconds which composed the year 2009. On the average, only about five out of the 60,000 calls were delayed for any reason, and even then the average delay was about two seconds. What cell phone network has that kind of reliability? How many times have you experienced "no service" or "call dropped" with your cell phone? Do we want firefighters who are reviving a heart attack victim and talking to the emergency room on the radio to all-of-a-sudden have their call dropped? Or should police

[3] See *Why Don't Cops Just Use Cell Phones?*, by Bill Schrier, September 10, 2010. http://www.digitalcommunities.com/blogs/city-cio/Why-Dont-Cops-Just-Use-Cell-Phones.html

officers lose service when drunk drivers clog the roads and bars are closing at 2:00 AM because a cell phone company decides to do maintenance because "no one uses the network then"?

- Disasters. Even small disasters cause cell phone networks to collapse. In Seattle, we've had swat team actions or car accidents which have shut down a freeway. Suddenly cell phone service abruptly ceases in that area because EVERYONE is on their phone. A few years ago a rifleman was loose and shooting people in Tacoma Mall. Responding police and EMTs had communications because they had dedicated networks and frequencies, but again cell phone networks were overloaded and down. In a larger disaster such as an earthquake or hurricane (with associated evacuation of large cities), commercial networks will be overloaded or jammed for days by people trying to escape the affected areas. Do we want police and fire departments - or even transportation, electric utilities and public works departments - to be trying to use those same networks while they are responding to the disaster? I don't think so.
- Talk-around. A key feature of most government-operated networks is something called talk-around or simplex or "walkie-talkie" mode. In this mode, individual radios talk directly to each other, without using a radio or cell tower. This is very important at incident scenes - firefighters commonly use it at the scene of a fire, because the radios will operate at the scene even if there isn't a tower nearby. But this is NEVER a feature of cellular phone networks. If the cell tower is down or out of range, that cell phone in your hands is a useless lump of plastic. But the radios of public safety officers still work and will talk to each other even without the tower.
- Ruggedness. No firefighter in his/her right mind would fight a fire using a cell phone for communications. The heat, water, and ruggedness of the environment would quickly destroy the device. Yet most public safety radios will survive being dropped repeatedly on the ground or being immersed in water for 30 minutes or more. No standard cell phone can survive the rigorous work of firefighting or policing.

NPSTC concurs with Mr. Schrier's assessment. The factors noted in his article and incorporated above are faced not only in Seattle, but by public safety responders across the country. Accordingly, NPSTC urges the Commission to consider the impact public safety requirements have on equipment design, price and choice by public safety entities. Clearly, while the use of cell phones and commercial networks may be viable for administrative activity and may be less expensive on the surface, they are not a substitute for dedicated mission critical public safety communications networks and radios designed to operate in the public safety environment.

Prior to the P25 standard, equipment manufacturers' analog trunked systems were built on proprietary platforms and were incompatible. To enable competition and interoperability as the industry moved to digital, the public safety community defined its requirements in the P25 Steering Committee and TIA with the help of TIA member manufacturers developed the P25 suite of

standards. An important element for interoperability in this suite of standards is the capability for backward compatibility, as public safety systems are not replaced overnight. The P25 standard was developed under ANSI guidelines, which provide for input and information sharing by multiple manufacturers that wish to participate in the development of the standard. Further, the approved standards documents are available to all manufacturers who want to develop P25 equipment. Therefore, the standard and the process under which it is developed enable any manufacturer that wants to commit resources to P25 development to do so. Over one dozen manufacturers now market P25 radios, as evidenced by the recent APCO conference and trade show which Commission officials attended.[4] NPSTC is aware of the need for additional education regarding P25 competition within the public safety community and pledges to help with that process.

Interoperability in the current public safety market has also benefitted from a number of other actions. The P25 Compliance Assessment Program (CAP) implemented by DHS and NIST formalizes interoperability, conformance and performance testing in recognized labs that was previously conducted only informally by some manufacturers. As addressed in the briefing to the FCC on September 2 by Dereck Orr, the CAP program has resulted in 8 accredited laboratories and multiple P25 products from multiple manufacturers having passed the CAP testing. When the test is completed, the vendor develops documentation called a Supplier's Declaration of Compliance (SDoC), and a Detailed Test Report. These documents are submitted to the DHS compliance program for review, and ultimate posting on a Responder Knowledge Base (RKB) website maintained by FEMA. Public safety users can access this site to learn what vendors have been validated to interoperate on which features with which other vendors. The SDoC identifies the

[4] http://www.project25.org/images/stories/ptig/docs/P25_PTIG_Equipment_Mfrs_2010-August.pdf

product or system and all of the subscriber radios tested with it. The current listing of the multitude of products tested by the program can be found on the FEMA RKB site.[5]

Additional elements of the P25 CAP program are also under development by NIST and DHS. For example, CAP testing of the P25 inter-system interface (ISSI) will formalize and expand testing for conformance and interoperability that has been successfully conducted informally by several P25 manufacturers in the public safety market.

In addition, interoperability improvements, both in communications system deployments and in governance, have been made as a result of the PSIC grant program. A number of jurisdictions are utilizing the PSIC grant funds to deploy updated and expanded communications systems to meet their current mission critical requirements. Some public safety experts in NPSTC served as peer-reviewers for PSIC grant applications.

While advances have been made, some point to the imperfection of interoperability in the public safety market. The P25 standard is based on public safety user requirements and those requirements are not ubiquitous across all public safety agencies. Therefore, the P25 standard incorporated optional features in addition to required elements. Given different operational requirements, not all public safety agencies choose to implement exactly the same set of features. The result is that not every element of one public safety P25 system is totally compatible with those of another agency's or jurisdiction's system.

Also, given the longevity of public safety systems, there are still systems in place, especially in the VHF and UHF bands, that operate only in the analog mode.[6] While P25 radios include an analog mode for backward compatibility, interoperability between an older analog system and a P25

[5] See https://www.rkb.us/

[6] Under Commission rules, P25 interoperability is required only in the 700 MHz band.

system that incorporates both analog and digital obviously depends on the mode of operation the agency with the P25 system chooses at a given incident. P25 provides additional features and 12.5 kHz efficiency in spectrum congested areas that an agency may prioritize for their operation.

In the VHF and UHF bands, the requirement to narrowband to 12.5 kHz channels by January 1, 2013, may have interoperability implications for some users. NPSTC is on record supporting the January 1, 2013, narrowbanding deadline and reaffirms that support. We believe the Commission's recent Stay of some elements of the interim deadlines that had been requested by NPSTC, for example, the ability to continue purchasing dual mode 25 kHz/12.5 kHz radios until January 1, 2013, will also help minimize transitional interoperability issues. There are concerns however, that have been expressed by public safety representatives, that interoperability could be hampered as some agencies implement narrowbanding on a different schedule than their neighbors. NPSTC urges the Commission to help ensure that its narrowbanding requirements are well understood by all public safety agencies. NPSTC recommends the Commission expeditiously implement an education program similar to the one it conducted to help remove wireless microphones from the 700 MHz band.

The 2013 VHF/UHF narrowband requirements relate to user operation with a 12.5 kHz or equivalent efficiency which can be accomplished with either digital or analog technology. While there are no user implementation requirements yet in these bands for a 6.25 kHz or equivalent efficiency, the Commission rules do require that equipment receiving FCC certification after January 1, 2013, includes a 6.25 kHz or equivalent efficiency mode. As a practical matter, this 6.25 kHz or equivalent efficiency mode will require the use of digital modulation. If/when the Commission requires users actually to deploy 6.25 kHz or equivalent efficiency equipment, a standard requirement similar to that done at 700 MHz will be needed for mutual aid channels in the

VHF/UHF band. Otherwise, a 6.25 kHz efficiency requirement will simply undercut interoperability.

Moving Forward with Broadband

Looking forward to broadband competition and interoperability, public safety and multiple members of the manufacturing community have all endorsed LTE as the technology of choice to enable interoperability. LTE will leverage the commercial equipment volumes in the 700 MHz band. The Commission specified LTE in its May 12 waiver Order, and NPSTC urges it to do so in any subsequent waiver grants and any changes to the rules. As all standards are periodically updated with additional revisions or "releases" as termed in the LTE standard, the Commission needs to develop an approach that allows public safety users to deploy future releases of the LTE standard as long as they include backward compatibility to previous releases to maintain interoperability. A Commission process that requires two or more years at minimum to modify even the most minor elements of a rule is simply not compatible with the rapid improvements of technology development in the market today.

All elements that affect competition and equipment pricing have tradeoffs. While LTE broadband equipment is driven by the higher volumes of the consumer and commercial market and therefore is expected to be less expensive, the LTE standards process is also driven by commercial and consumer needs. Therefore, public safety is unlikely to have the same high level degree of influence in defining future elements of the LTE standard as it has had in the development of P25. In deploying broadband, public safety will still require the availability of devices which are ruggedized and meet public safety operational requirements that are often unique from those of consumers and commercial providers.

NPSTC urges the Commission to utilize the combined expertise of the public safety community, equipment manufacturers, DHS, and NIST to help address standards important to the public safety community in the 3GPP standards process that defines LTE standards. We believe this is an appropriate issue to be addressed in ERIC, but it should not delay deployment by those with 700 MHz broadband waivers. There is much that public safety and the Commission can learn through such waiver deployments.

The Public Notice indicates the Commission wants to examine all potential barriers to achieving nationwide interoperability for both broadband and narrowband communications, and determine what, if any, actions the Commission should take in this area. A key area that has impacted interoperability in the current public safety market for years and will continue to do so as broadband is deployed is the availability of spectrum. Unlike the equipment market, which has multiple suppliers, there is only one supplier of public safety spectrum – the Commission. Therefore Commission decisions, which can be guided by Congress, have a key impact on interoperability.

Commission decisions can be very positive for interoperability or can have negative impacts. For example, as evidenced by recent filings with the Commission, the designation of the narrowband 700 MHz spectrum is an essential resource, especially for those who are out of channels in the adjacent 800 MHz band. In contrast, past decisions over 50 years that have resulted in insufficient piecemeal spectrum allocations have had a huge negative affect on interoperability, often requiring public safety officials to carry multiple radios. The current public safety equipment market must provide products that collectively operate over multiple small slivers of spectrum across the VHF, UHF, T-Band, 800 MHz, and 700 MHz bands. While the recent provision of

multi-band radios can address this situation over time, the imbedded base of single band radios will be in the market for years to come.

As public safety, the Commission, and industry embark on broadband, it is extremely important to learn from the past and to provide sufficient contiguous spectrum to accommodate public safety needs, both current and foreseeable. For that reason, the public safety community is united in its pursuit of the D block spectrum for 700 MHz public safety broadband, a position NPSTC fully supports. NPSTC believes that dedicating sufficient contiguous spectrum is the single most important step the Commission and Congress can take to set the foundation for interoperability in the nationwide broadband network. Without sufficient spectrum to accommodate public safety broadband needs and growth, all the other elements required, e.g., a common standard, interoperability plans, collaborative governance, etc., will be hampered from the outset.

NPSTC previously set forth a framework for interoperability in its Broadband Task Force (BBTF) and is pleased to see that the Commission adopted a number of the BBTF recommendations in the waiver grant Order.[7] NPSTC believes the framework provided in the BBTF is the right approach and will serve as a basis for future rule changes. However, any FCC detailed requirements on specific applications and governance aspects of interoperability could be postponed until systems are in place and there is at least some preliminary operational experience on what works best. A significant advantage to being very selective on rule requirements, while deferring as many issues as possible to PSST or ERIC guidelines, is the ability to adjust based on experience without the multi-year process needed to make rule changes.

[7] Order, Docket 06-229, released May 12, 2010.

Conclusion

NPSTC appreciates the opportunity to provide input on these important issues. Significant public safety expertise resides in NPSTC and we look forward to working with FCC, ERIC, PSST, PSCR, DHS, and industry in defining the path forward so public safety has the best possible options to meet its needs.

Respectfully submitted,

Ralph A. Haller, Chair

National Public Safety Telecommunications Council

8191 Southpark Lane, Number 205

Littleton, Colorado 80120-4641

866-807-4755

September 20, 2010